Lab 187

Morris & Opazo

aws re/start

Trabajo con AWS CloudTrail

INTRODUCCIÓN

AWS CloudTrail permite realizar auditorías, supervisar la seguridad y solucionar problemas operativos mediante el seguimiento de la actividad del usuario y el uso de la API . CloudTrail registra, supervisa de forma continua y conserva la actividad de la cuenta relacionada con las acciones en toda su infraestructura de AWS, lo que le permite controlar el almacenamiento, el análisis y las acciones de reparación.

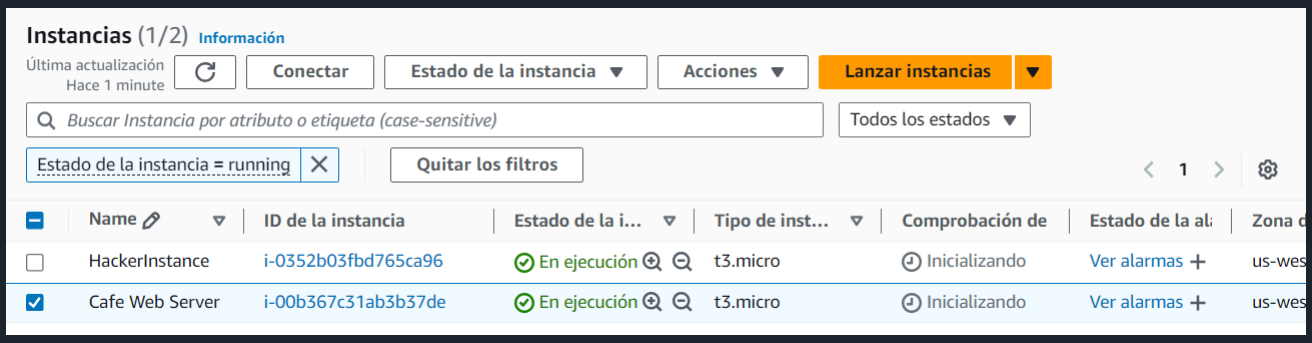
OBJETIVOS

- Crear y Configurar un rastro de CloudTrail.
- Analice los registros de CloudTrail mediante varios métodos para descubrir información relevante.
- Importar datos de registro de CloudTrail a Athena.
- Ejecutar consultas en Athena para filtrar las entradas de registro de CloudTrail.
- Resolver problemas de seguridad dentro de la cuenta de AWS y en una instancia EC2 de Linux.

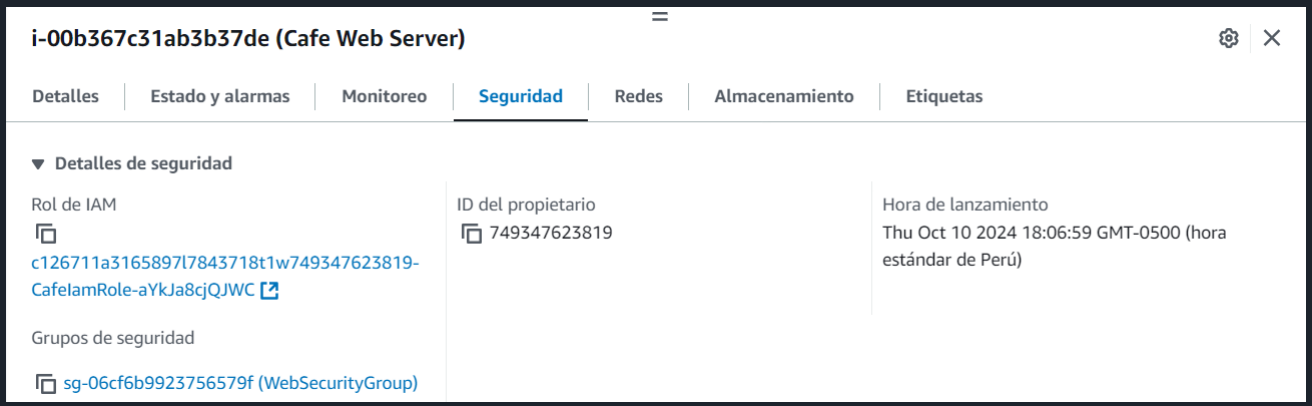
TAREA 1

En esta se procede a modificar un grupo de seguridad y observar el sitio web.

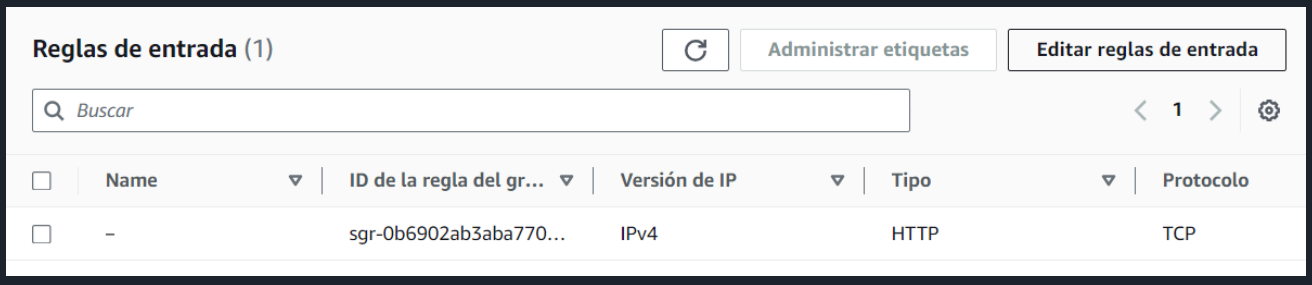
- EnDesde el menú Servicios, seleccione Computación y luego el servicio EC2.
- Seleccione Instancias y luego localice y seleccione la instancia Café Web Server (WebSecurityGroup).



- En la pestaña Seguridad, elija el grupo de seguridad sg-xxxxxxxxxx.

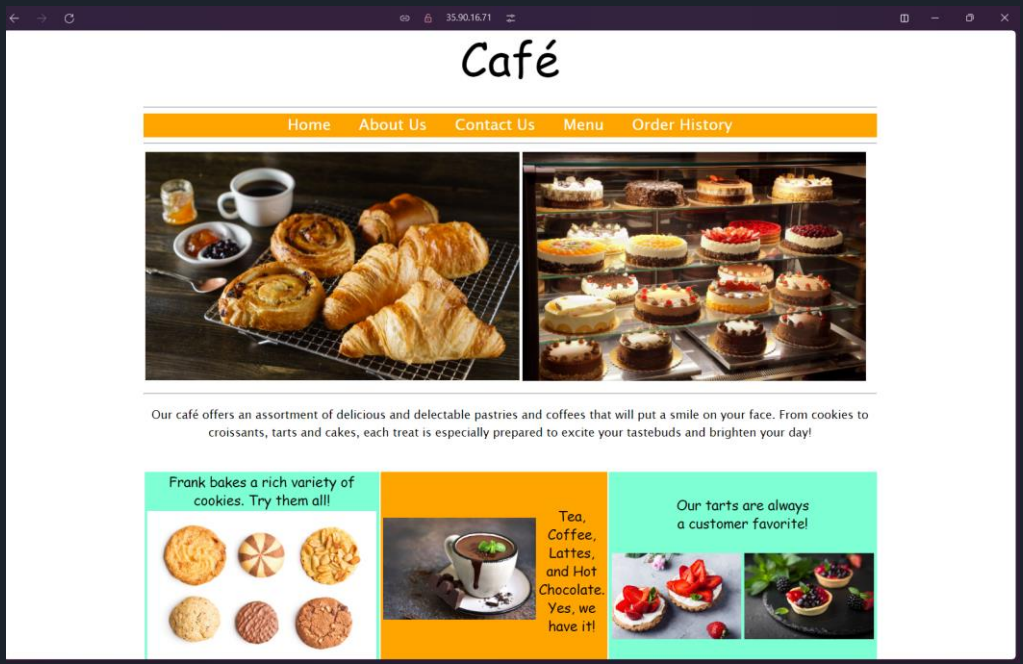


- En la pestaña Reglas de entrada, observe que solo se ha definido una regla de entrada, que es para el acceso HTTP a través del puerto TCP 80.



- Seleccione Editar reglas de entrada y luego seleccione Agregar regla y configure la regla de la siguiente manera:

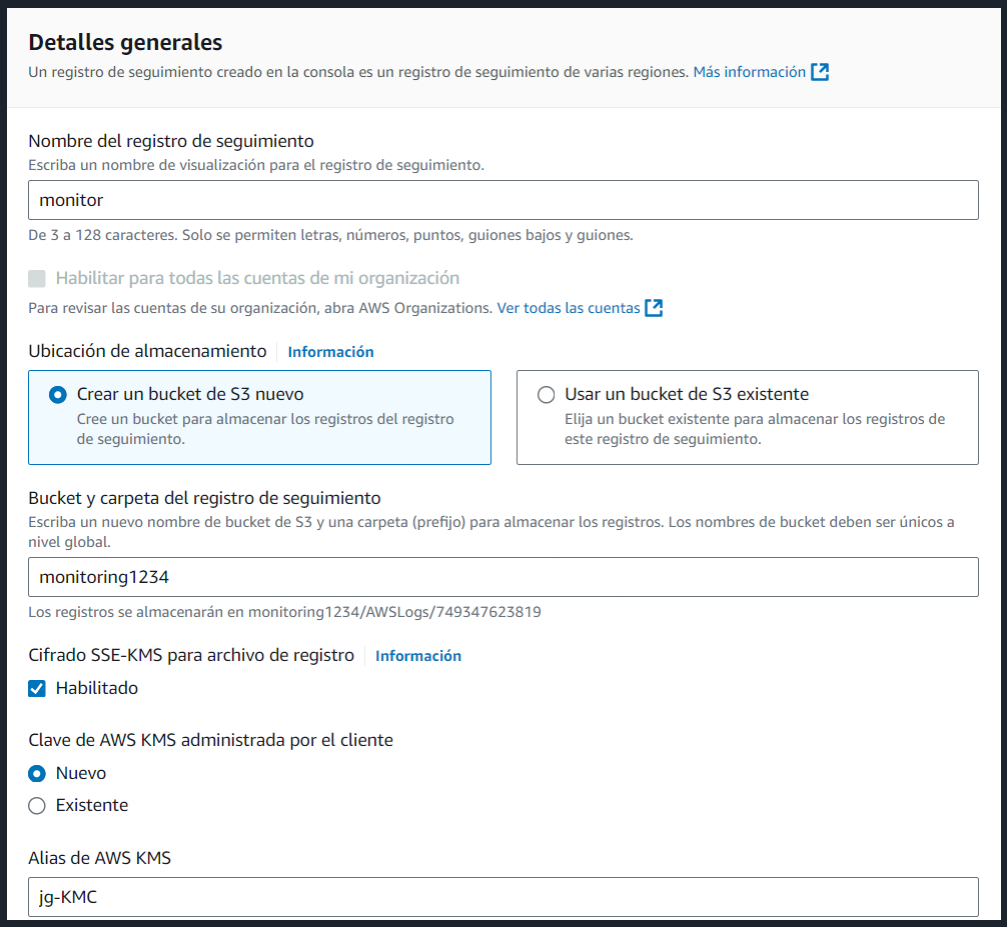
- En la parte inferior de la página, seleccione Guardar reglas.
- Consulte el sitio web del Café:



TAREA 2

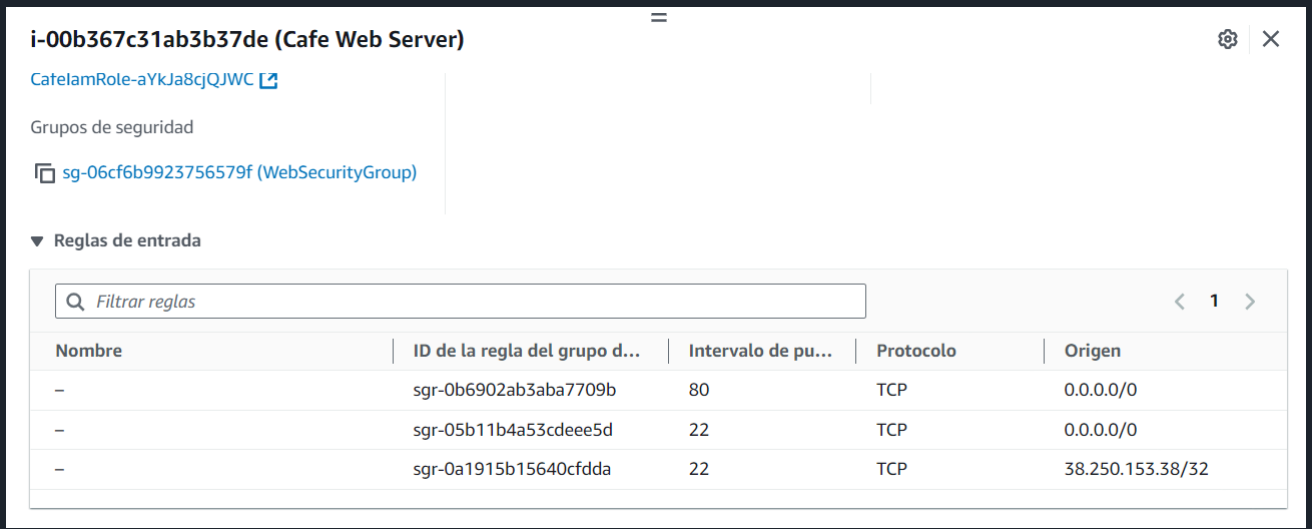
En esta tarea, creas un rastro de CloudTrail en tu cuenta de AWS. También notas que, poco después de crear el rastro, el sitio web de Café es hackeado.

- En la consola de administración de AWS, en el menú Servicios, seleccione Administración y gobernanza y, luego, CloudTrail. Ignore el mensaje de acceso denegado a AWSOrganizations que aparece en la parte superior de la consola.
- En el panel de navegación de la izquierda, seleccione Senderos.
- Seleccione Crear ruta.
- Configure la ruta de la siguiente manera:



- Elija Siguiente.
- En la página Elegir eventos de registro, seleccione Siguiente
- En la página Revisar y crear, seleccione Crear ruta
- Verifica que veas tu sendero en la página Senderos.
- Regrese a la pestaña del navegador donde tiene abierto el sitio web de Café y actualice la página.

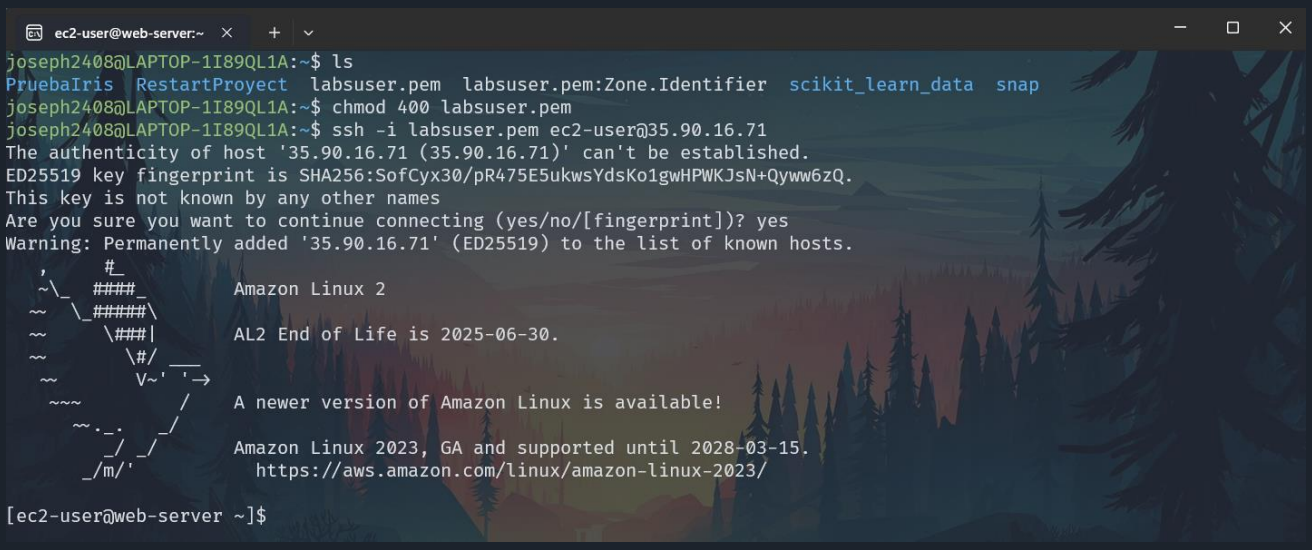
- En la consola de administración de AWS, navegue hasta el servicio EC2 y observe los detalles de la instancia del servidor web Café.
- En la pestaña Seguridad, elija nuevamente el grupo de seguridad sg-xxxxxxxxxx y luego elija la pestaña Reglas de entrada.



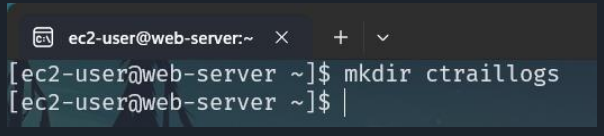
TAREA 3

En esta tarea, analizará los registros de CloudTrail utilizando la utilidad grep de Linux para ver si puede descubrir quién pirateó el sitio web.

- Ingresar a AWS mediante SSH.
- Verifique que su terminal esté conectada vía SSH a la instancia EC2 de Café Web Server.

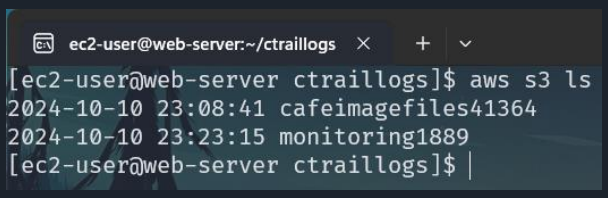


- Ejecute el siguiente comando para crear un directorio local en el servidor web para descargar los archivos de registro de CloudTrail:

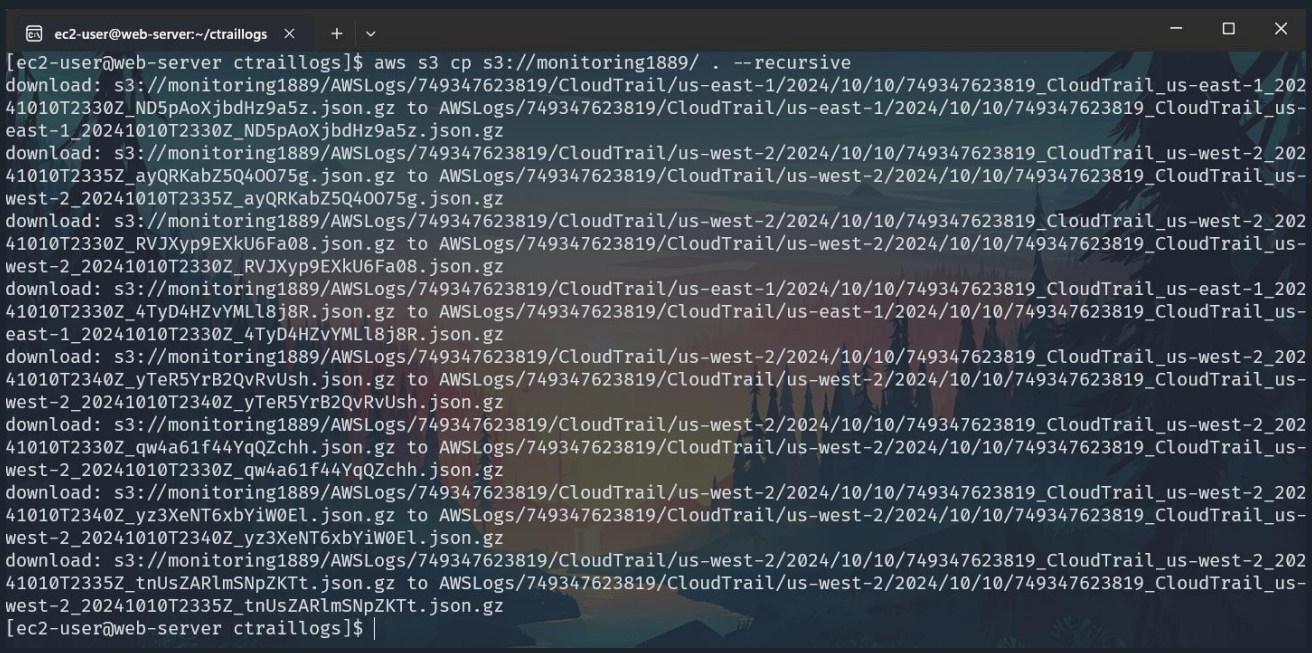


- Ejecute el siguiente comando para cambiar el directorio al nuevo directorio:

- Ejecute el siguiente comando para enumerar los depósitos y recuperar el nombre del depósito:

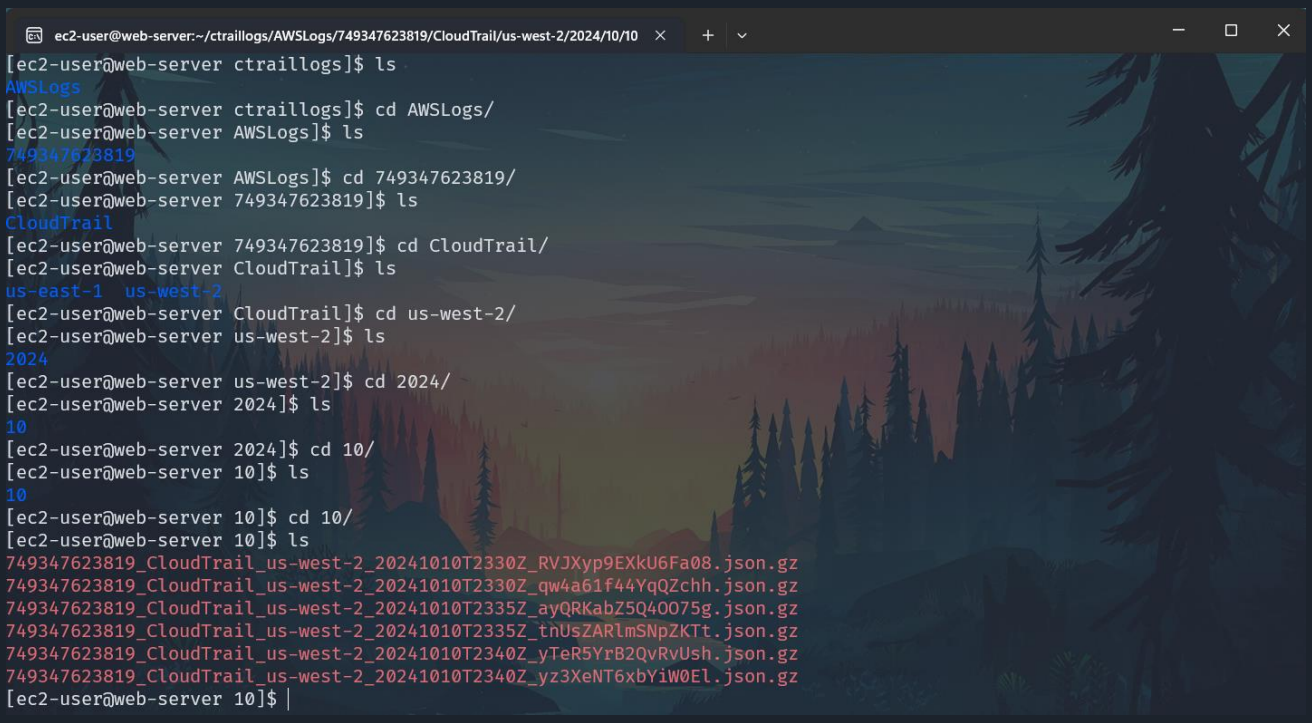


- En el siguiente comando, reemplace <monitoring#### > con el nombre del depósito real que comienza con monitoring (el nombre del depósito es parte del resultado del lscomando que ejecutó). Ejecute el comando modificado para descargar los registros de CloudTrail:

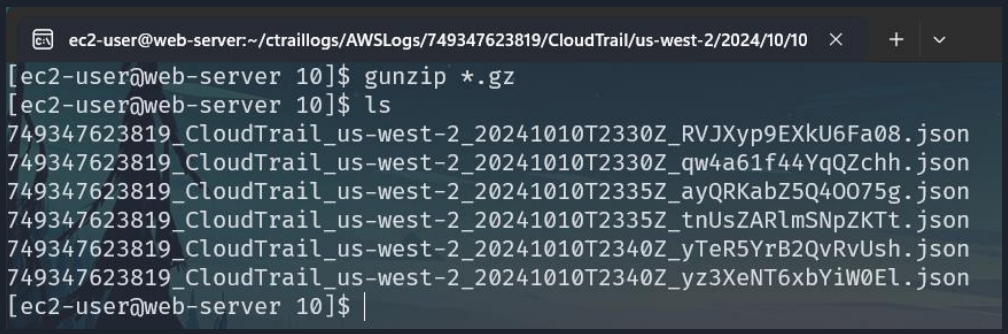


- Utilice los comandos cdy lsrepetidamente (o ingrese cdy luego presione Tab varias veces) según sea necesario para cambiar el directorio al subdirectorio donde se descargaron los registros. Cuando ejecute ls, se deben mostrar todos los archivos de registro descargados. Se ubicarán en un

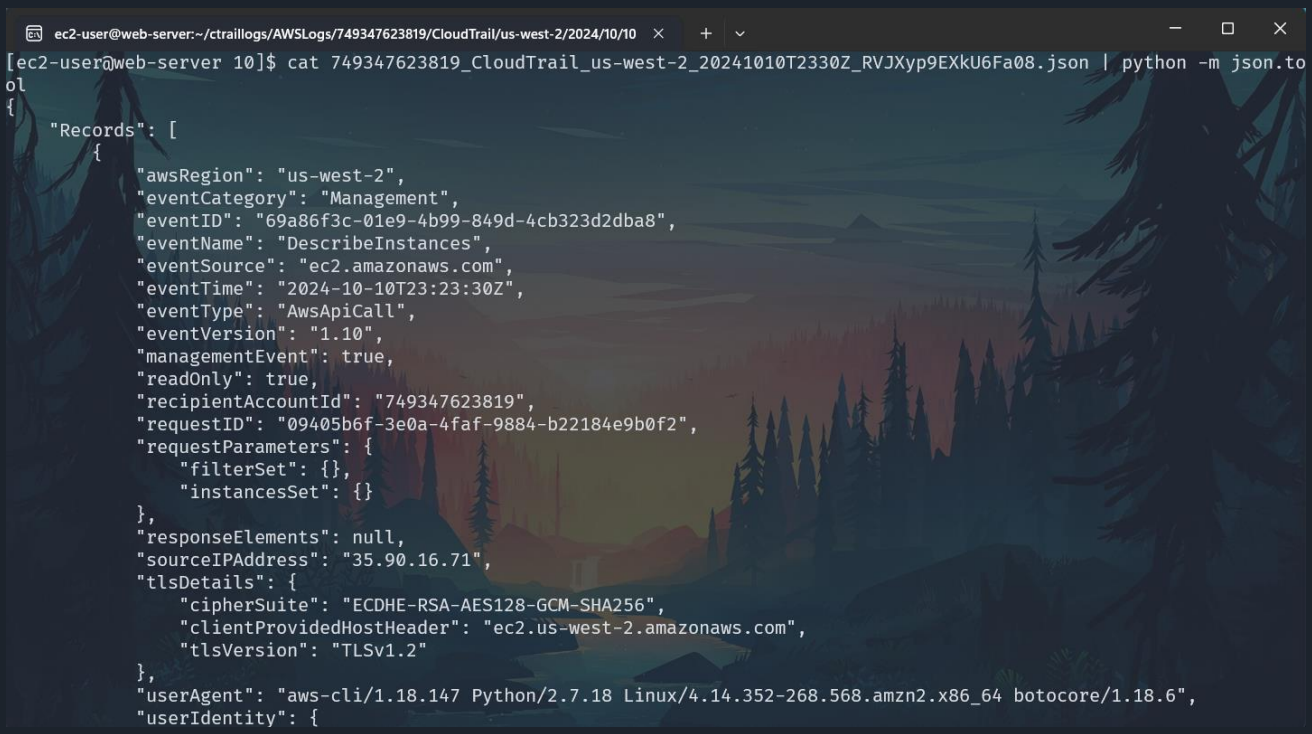
subdirectorio AWSLogs/ < account-num > /CloudTrail/ < Region > / < yyyy > / < mm > / < dd >.



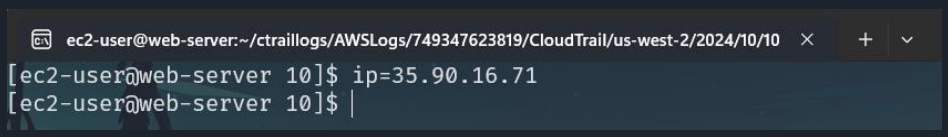
- Ejecute el siguiente comando para extraer los registros:
- Ejecute ls nuevamente. Observe que todos los archivos ya están extraídos.



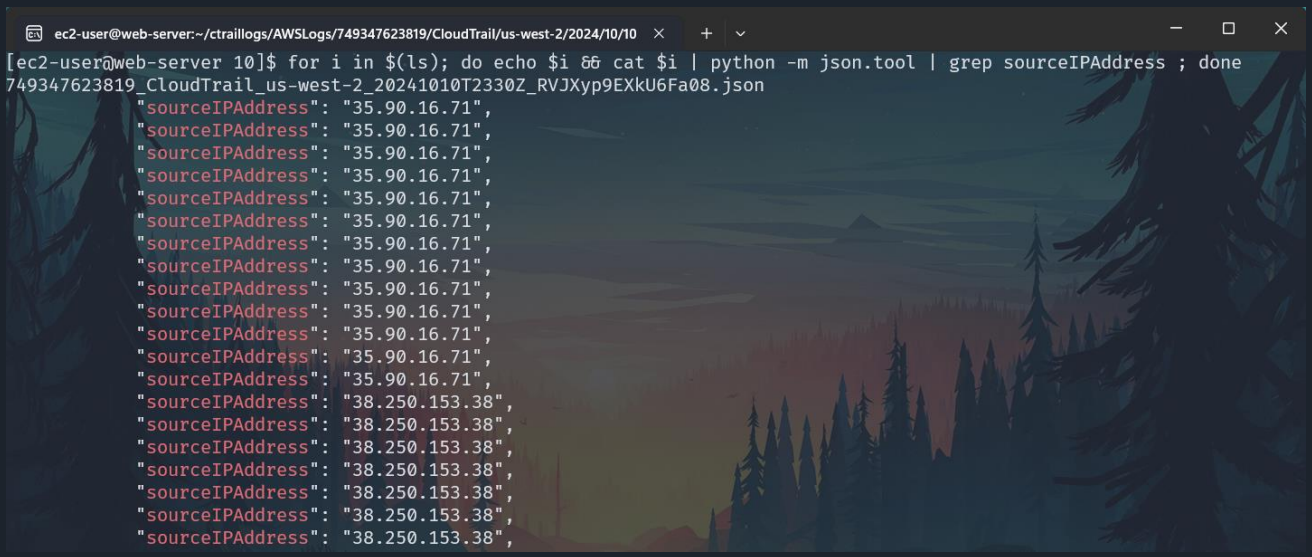
- Para analizar la estructura de los registros, haga lo siguiente:



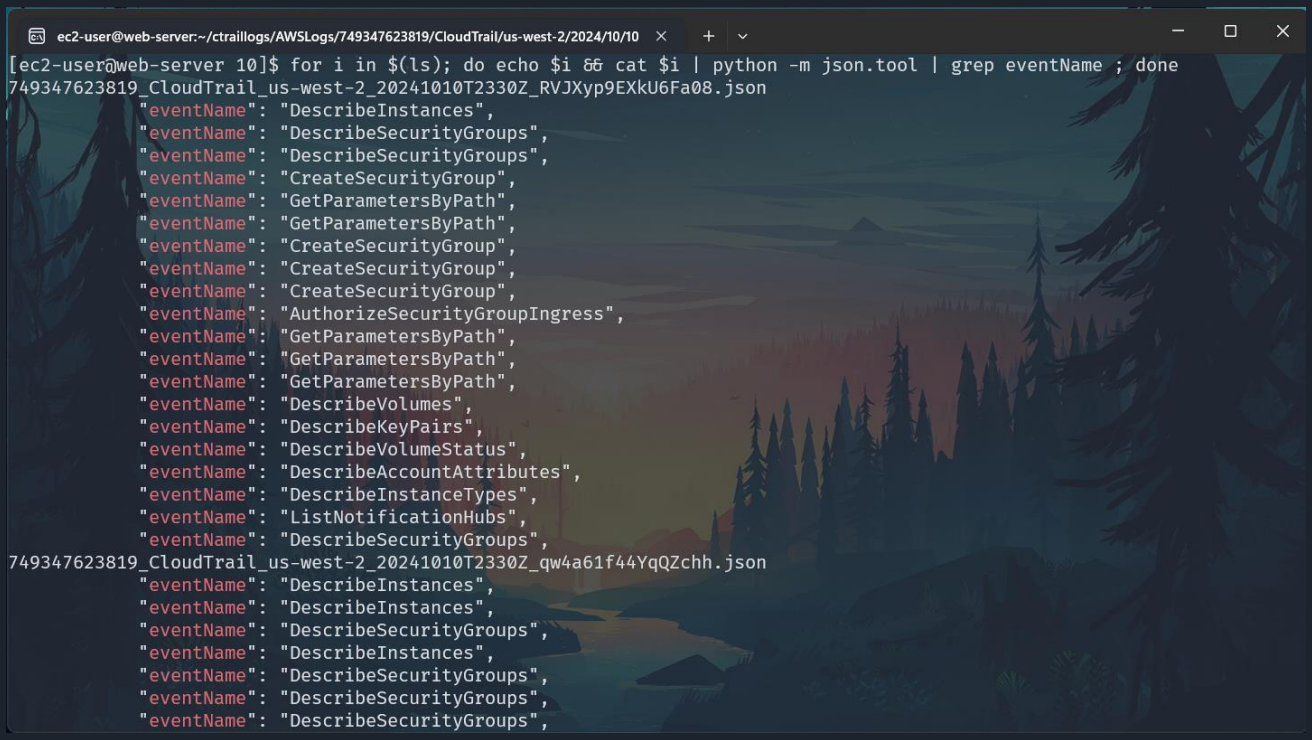
- Ejecute el siguiente comando para establecer la dirección WebServerIP como una variable que puede usar en comandos futuros (reemplace < WebServerIP > con la dirección IP real que se muestra a la izquierda de estas instrucciones):



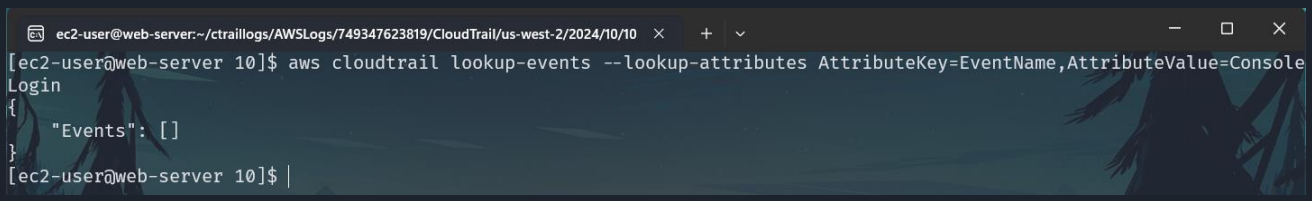
- Ejecute el siguiente comando:



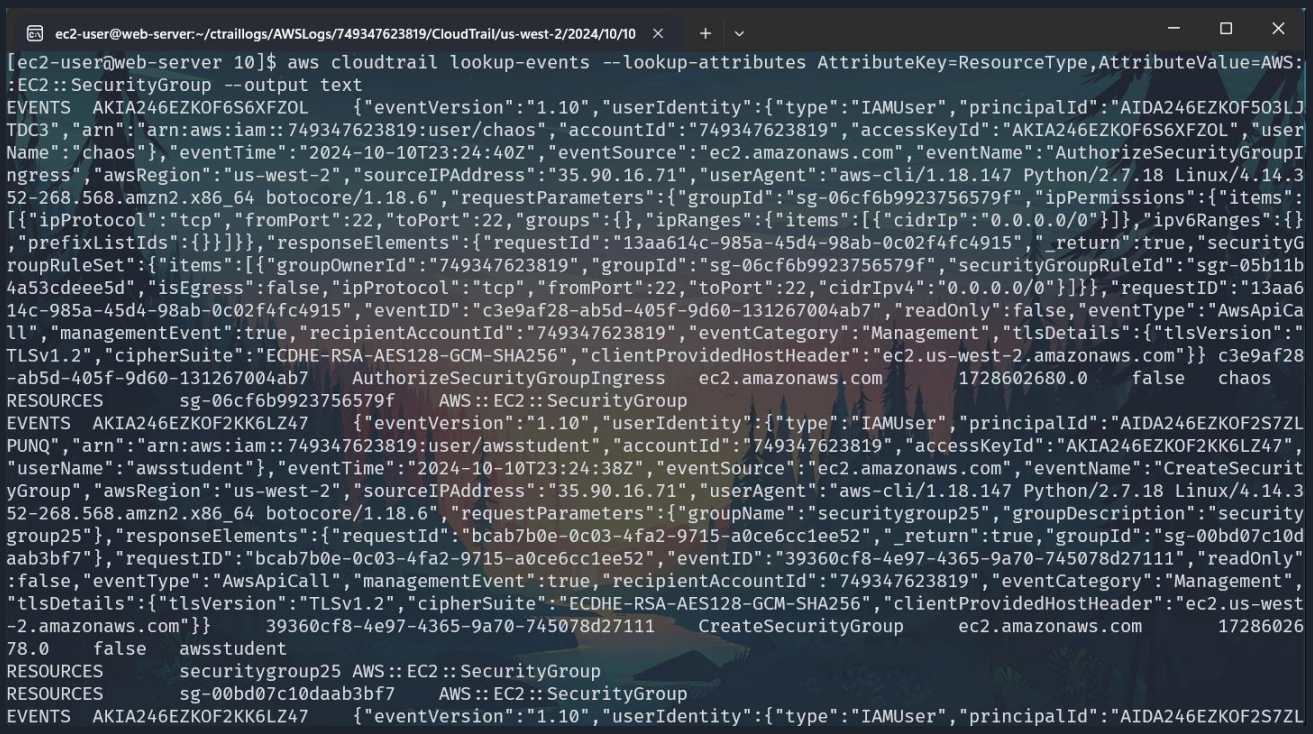
- Ejecute un comando con una estructura similar pero donde el comando devuelva el eventName de cada evento capturado:



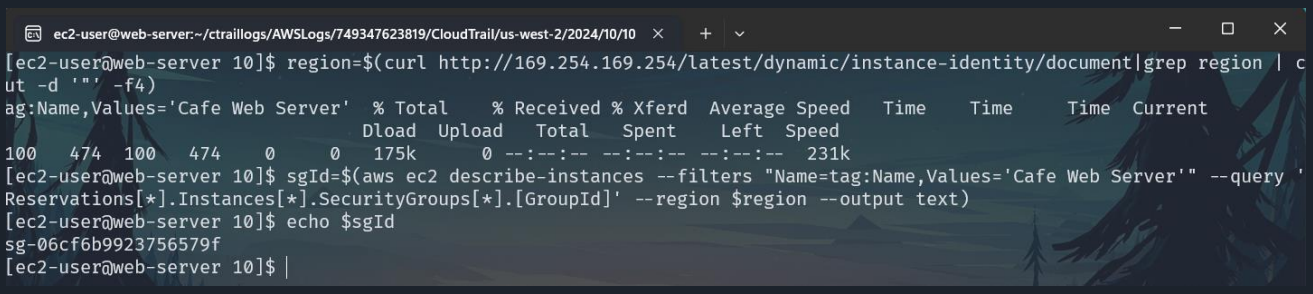
- Abra la página de referencia de AWS CLI para CloudTrail.
- Elija el comando lookup-events para ver detalles sobre el comando.



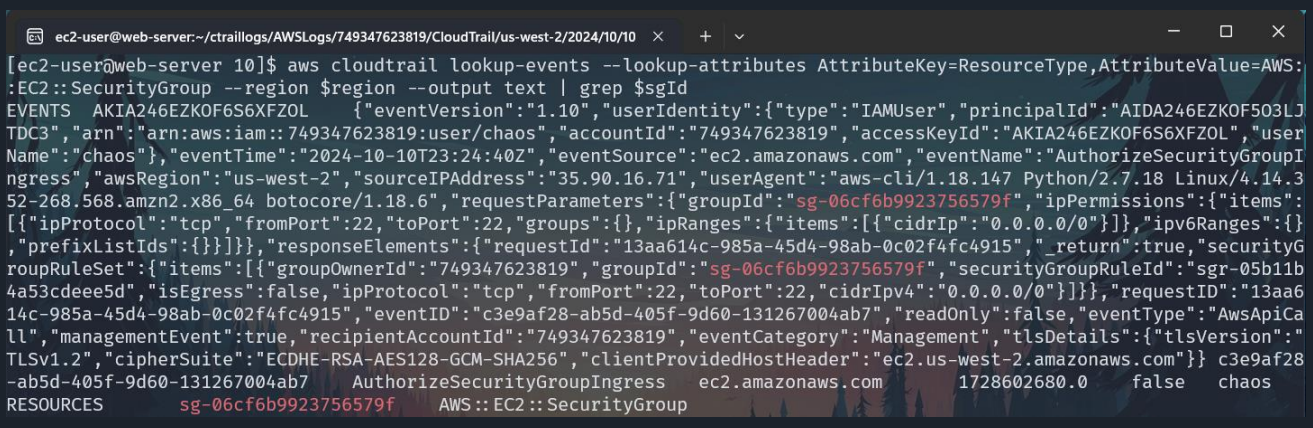
- Ejecute el siguiente comando para encontrar las acciones que se realizaron en los grupos de seguridad en la cuenta de AWS:



- Ejecute los siguientes comandos para encontrar el ID del grupo de seguridad que utiliza la instancia del servidor web Café y luego repita el resultado en la terminal:



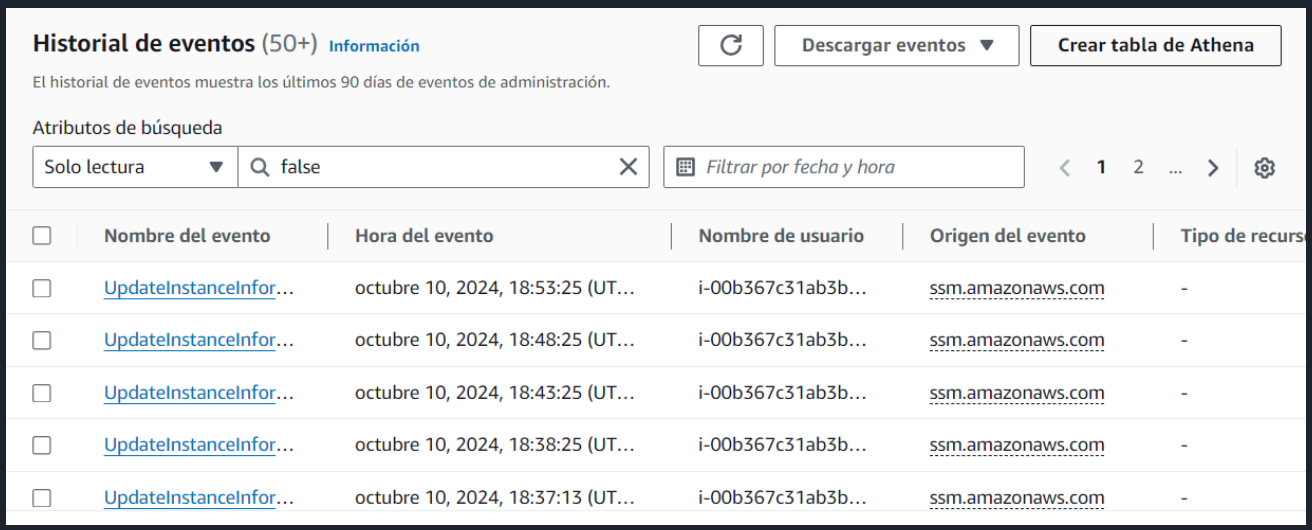
- Ahora use el ID del grupo de seguridad que devolvió el comando anterior para filtrar aún más los resultados del comando CloudTrail de AWS CLI:



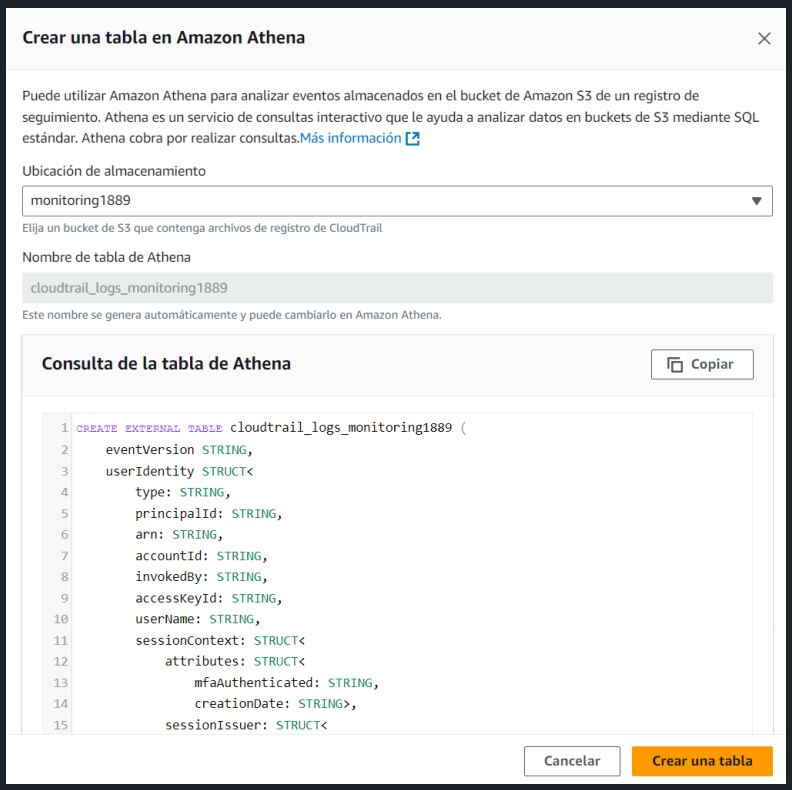
TAREA 4

En esta tarea, utilizará Athena para analizar sus registros de CloudTrail.

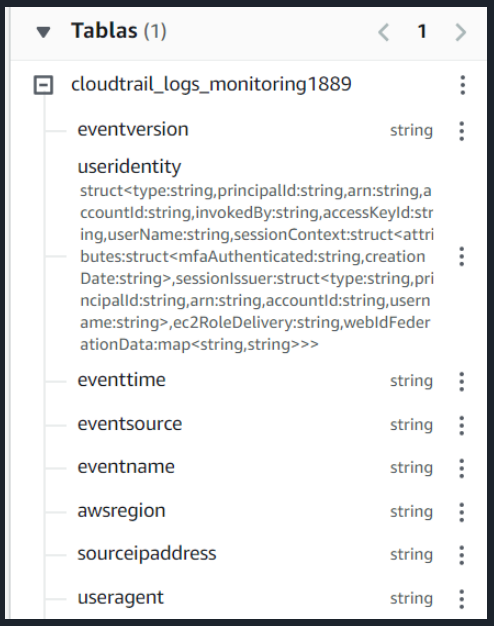
- Desde el menú Servicios de la consola de administración de AWS, elija CloudTrail para abrir la consola de CloudTrail.
- En el panel de navegación, seleccione Historial de eventos.
- Desde la página Historial de eventos, haga clic en Crear tabla de Athena.
- Tómese un momento para analizar cómo se forma la declaración CREATE TABLE de Athena.



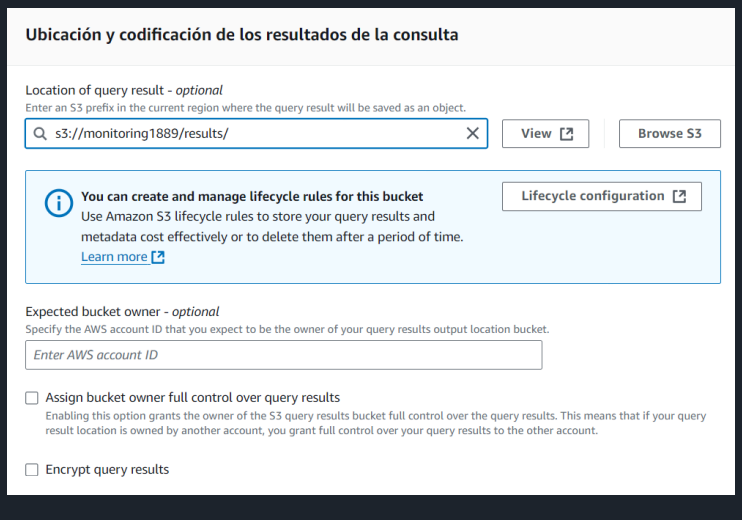
- Una vez que haya terminado de analizar los detalles de CREAR TABLA, seleccione Crear tabla.

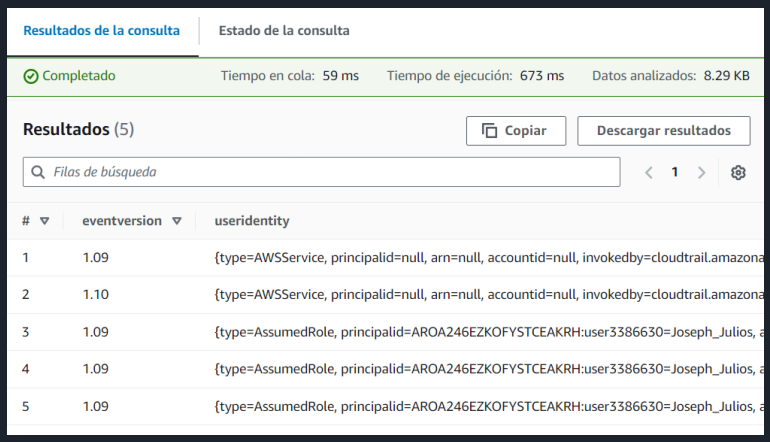


- Desde el menú Servicios, seleccione Análisis y luego el servicio Athena.
- Si aún no ve el Editor de consultas de Athena, seleccione Explorar editor de consultas y debería aparecer.
- En el panel izquierdo del Editor de consultas de Athena, debería ver la tabla cloudtrail_logs_monitoring####.

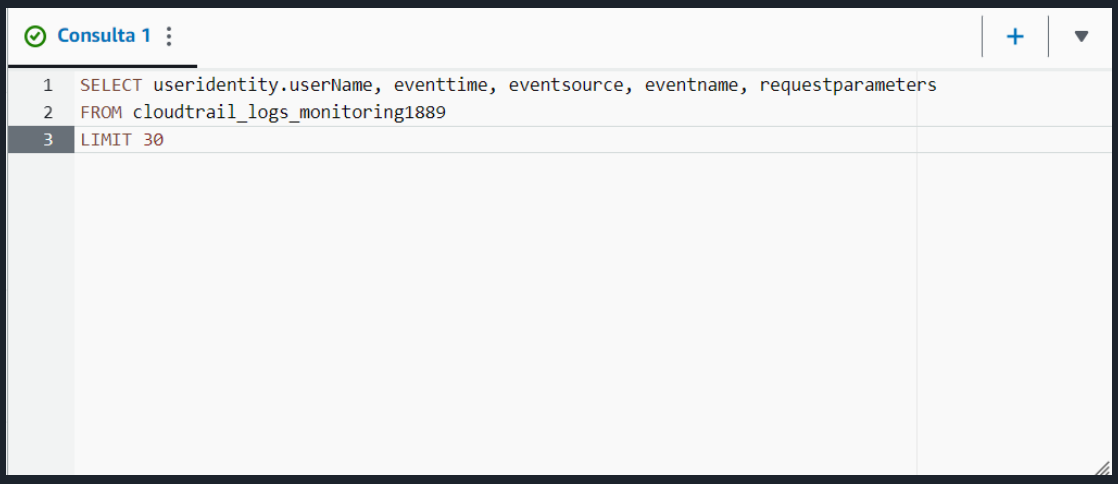


- Comience configurando una ubicación para los resultados de la consulta y luego ejecute una consulta simple para tener una idea de los datos que están disponibles en los registros.





- Ejecute una nueva consulta que seleccione únicamente las columnas mencionadas anteriormente. Esta vez, limite los resultados a 30 filas:



Resultados de la consulta | Estado de la consulta

Completado | Tiempo en cola: 100 ms | Tiempo de ejecución: 661 ms | Datos analizados: 16.83 KB

Resultados (30)

Copiar | Descargar resultados

Filas de búsqueda

1

#	userName	eventtime	eventsource	eventname
1		2024-10-11T00:04:14Z	organizations.amazonaws.com	DescribeOrganization
2		2024-10-11T00:05:13Z	iam.amazonaws.com	ListRoles
3		2024-10-11T00:05:09Z	kms.amazonaws.com	GenerateDataKey
4		2024-10-11T00:05:09Z	s3.amazonaws.com	GetBucketAcl
5		2024-10-11T00:05:13Z	kms.amazonaws.com	DescribeKey
6		2024-10-11T00:05:13Z	athena.amazonaws.com	ListWorkGroups
7		2024-10-11T00:05:16Z	athena.amazonaws.com	ListDataCatalogs
8		2024-10-11T00:05:13Z	athena.amazonaws.com	ListWorkGroups
9		2024-10-11T00:05:16Z	athena.amazonaws.com	ListQueryExecutions

Desafío: Identifica al Hacker

En esta sección de la actividad, intenta descubrir la entrada del registro que incluye la información esencial sobre quién hackeó el sitio web. No se proporcionan pasos específicos. En su lugar, debes experimentar ejecutando distintas consultas hasta que encuentres la información que estás buscando.

Consulta 1

```
1  SELECT DISTINCT useridentity.userName, eventName, eventSource FROM cloudtrail_logs_monitoring1889
       WHERE from_iso8601_timestamp(eventtime) > date_add('day', -1, now()) ORDER BY eventSource;
```

Resultados (93)

Copiar | Descargar resultados

Filas de búsqueda

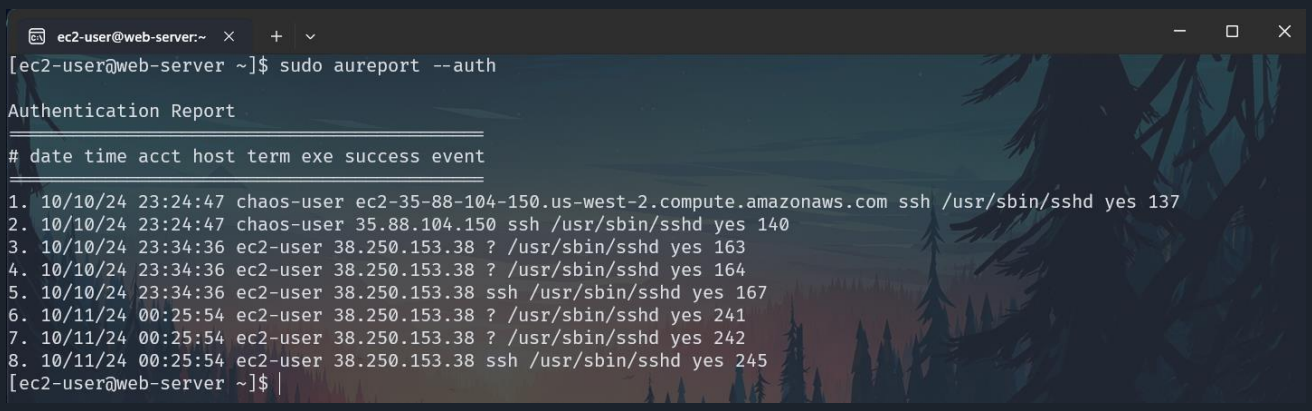
1

#	userName	eventName	eventSource
1		ListQueryExecutions	athena.amazonaws.com
2		ListDataCatalogs	athena.amazonaws.com
3		GetQueryRuntimeStatistics	athena.amazonaws.com
4		ListWorkGroups	athena.amazonaws.com
5		GetQueryExecution	athena.amazonaws.com
6		GetQueryResults	athena.amazonaws.com
7		StartQueryExecution	athena.amazonaws.com
8		BatchGetQueryExecution	athena.amazonaws.com
9		GetWorkGroup	athena.amazonaws.com
10		DescribeAutoScalingGroups	autoscaling.amazonaws.com

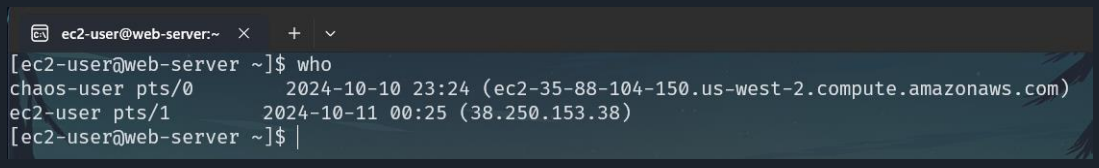
TAREA 5

En esta última tarea, trabajará para proteger tanto su cuenta de AWS como la instancia del servidor web.

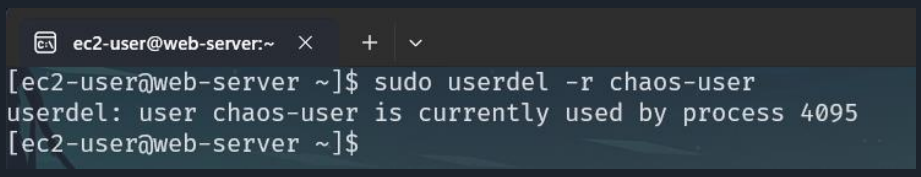
- En la terminal donde tiene una sesión SSH activa en la instancia del servidor web, ejecute el siguiente comando para averiguar quién ha iniciado sesión recientemente en este sistema operativo (SO):



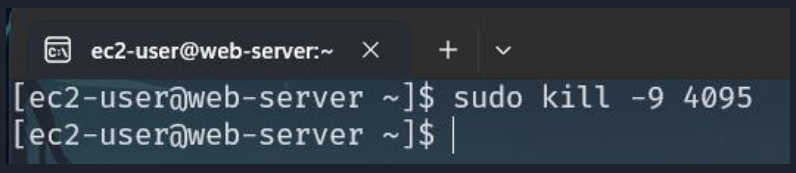
- Ejecute el comando who para averiguar quién está conectado actualmente:



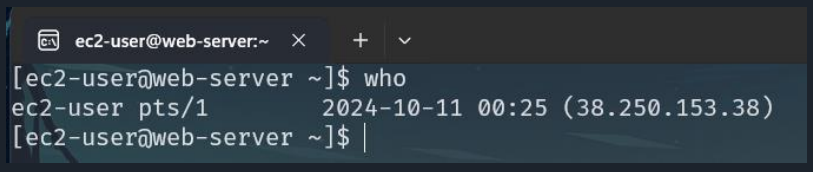
- Ejecute el siguiente comando para intentar eliminar el usuario del sistema operativo chaos-user:



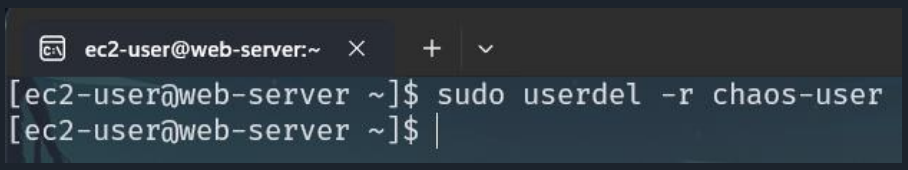
- En el siguiente comando, reemplace ProcNum por el número de proceso devuelto por el último comando. Ejecute el comando modificado para detener el proceso que tiene activa la sesión de inicio de sesión de usuario Chaos:



- Ejecute el comando who nuevamente para verificar que el usuario del sistema operativo chaos-user ya no esté conectado:



- Ejecute el siguiente comando para intentar eliminar el usuario chaos nuevamente:



- Ejecute el siguiente comando para verificar que no haya otros usuarios sospechosos del sistema operativo que puedan iniciar sesión:

```
ec2-user@web-server:~
[ec2-user@web-server ~]$ sudo cat /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
ec2-user:x:1000:1000:EC2 Default User:/home/ec2-user:/bin/bash
[ec2-user@web-server ~]$
```

- Analizar la configuración de SSH en la instancia.

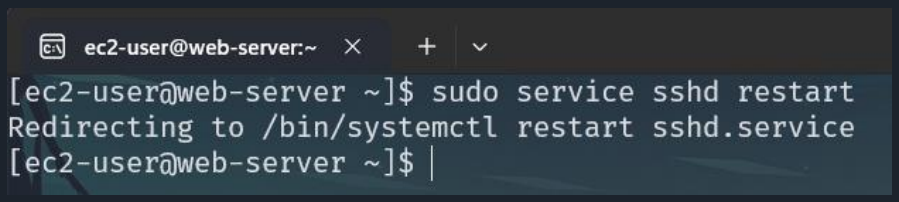
```
ec2-user@web-server:~
[ec2-user@web-server ~]$ sudo ls -l /etc/ssh/sshd_config
-rw------- 1 root root 3957 Oct 10 23:08 /etc/ssh/sshd_config
[ec2-user@web-server ~]$
```

- Ejecute el siguiente comando para editar el archivo de configuración SSH en el editor VI:

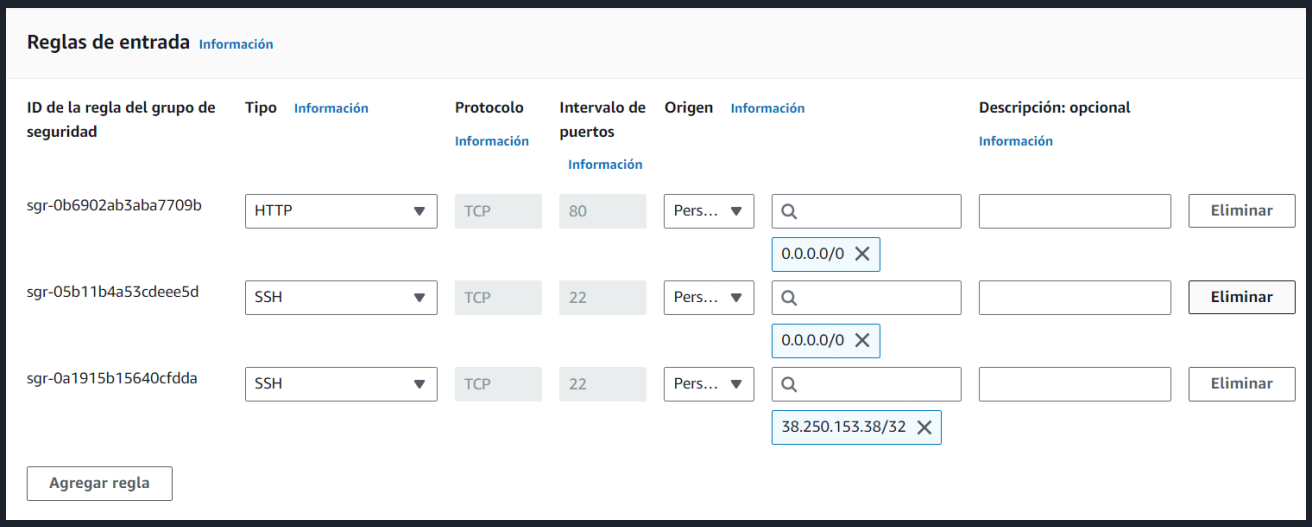
```
ec2-user@web-server:~
[ec2-user@web-server ~]$ sudo vi /etc/ssh/sshd_config
[ec2-user@web-server ~]$
```

```
ec2-user@web-server:~
#AuthorizedPrincipalsFile none


# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
                                                          63,1          43%
```

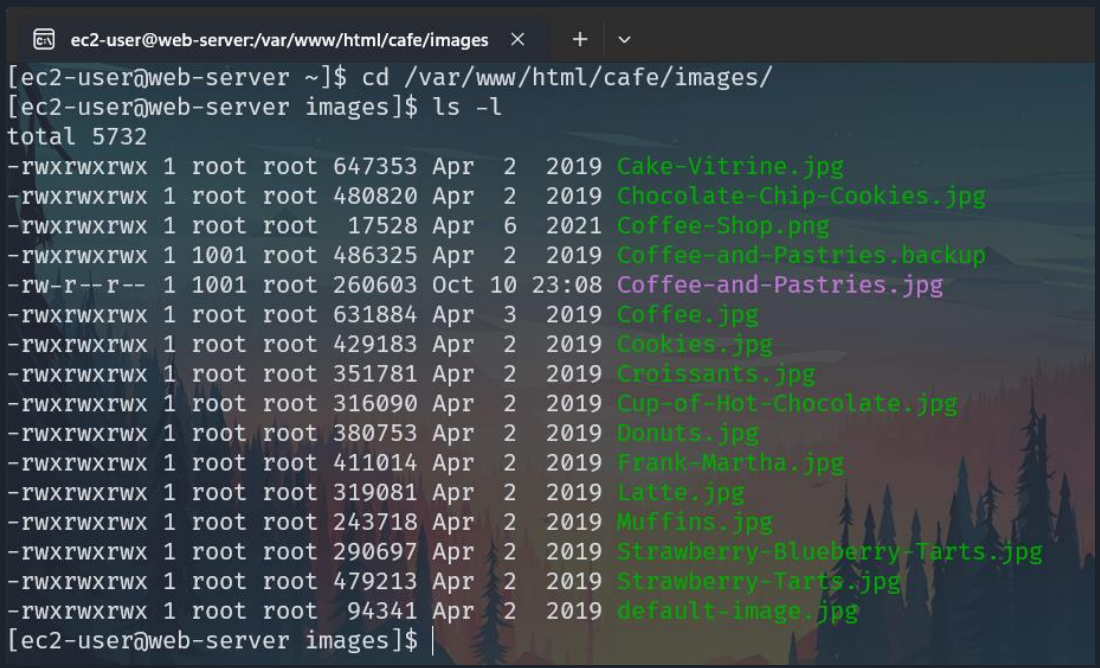
- Ejecute el siguiente comando para reiniciar el servicio SSH para que los cambios surtan efecto:



- Por último, en la consola EC2, regrese a la configuración del grupo de seguridad del servidor web. Eliminar SSH.



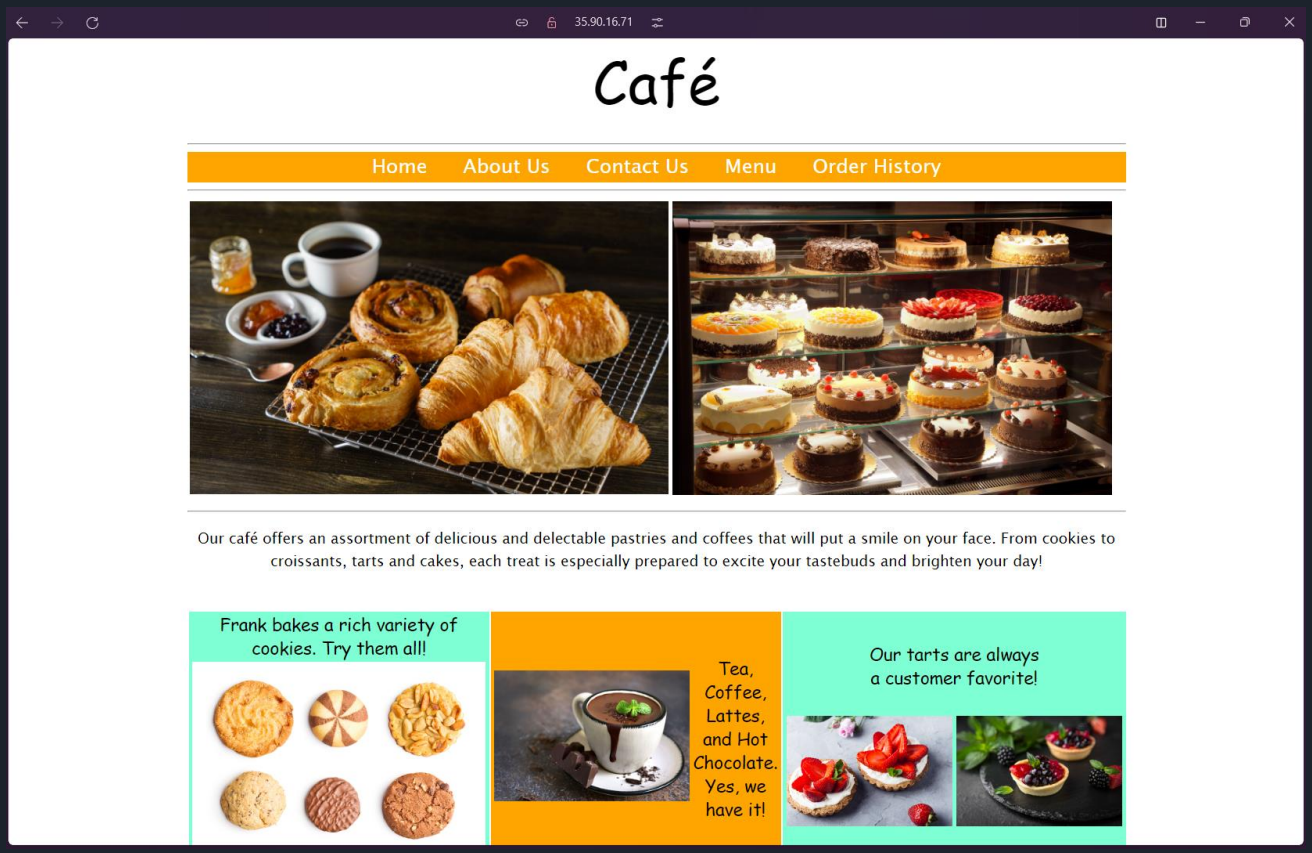
- Guarde el cambio.
- Ejecute el siguiente comando para navegar al directorio donde se encuentran los archivos de imagen del sitio web y revisar el contenido:



- Ejecute el siguiente comando para restaurar el gráfico original en el sitio web.

```
ec2-user@web-server:/var/www/html/cafe/images
[ec2-user@web-server images]$ sudo mv Coffee-and-Pastries.backup Coffee-and-Pastries.jpg
[ec2-user@web-server images]$
```

- Para probar la solución, vuelva a cargar el sitio web http://WebServerIP/cafe en el navegador.



- En la consola de administración de AWS, elija el menú Servicios y elija IAM.
- Seleccione el enlace Usuarios y seleccione la casilla de verificación junto al usuario Chaos.

- Seleccione Eliminar, ingrese el nombre del usuario y seleccione Eliminar.